12 FAM 590
CYBER SECURITY INCIDENT PROGRAM

(CT:DS-161; 03-01-2011)
(Office of Origin: DS/IS/APD)

12 FAM 591 GENERAL

12 FAM 591.1 Purpose

(CT:DS-124; 01-10-2007)

The purpose of the Cyber Security Incident Program (CSIP) is to enhance the protection of Department of State's cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cyber security. The CSIP focuses on accountability of personnel for actions leading to damage or risk to Department automated information systems (AISs) and infrastructure, even when only unclassified material or information is involved.

12 FAM 591.2 Responsibilities

(CT:DS-124; 01-10-2007)

a. The confidentiality, integrity, and availability of Department AISs are critical to the Department's operations. At posts abroad, the Deputy Chief of Mission (DCM), Charge, or Principal Officer or Consul General, as appropriate, is the ultimate owner of that portion of the Department's cyber infrastructure and is responsible for its security. Domestically, the Bureau Executive is considered the system owner (see 5 FAM 814 r). In both cases, system security functions are delegated to the information systems security officer (ISSO). AIS users must also share in this responsibility by strictly adhering to the Department's computer security policy.

b. The Department's computer security policies are codified throughout 5 FAM and 5 FAH, as well as in 12 FAM 600. Any questions regarding these policies should be addressed to DS/SI/CS via e-mail at ASKCS@state.gov.

12 FAM 591.3 Applicability

(CT:DS-124; 01-10-2007)

The CSIP applies to all Department AIS users including those users who do not possess security clearances.

12 FAM 591.4 Authorities

(CT:DS-124; 01-10-2007)

a. Relevant legal authorities include:

(1) Federal Information Security Management Act (FISMA)(2002);

(2) Computer Fraud and Abuse Act (1984), as amended by the United States of America Patriot Act of 2001;

(3) Privacy Act of 1974; and

(4) Executive Order 13231, Critical Infrastructure Protection in the Information Age (2001), February 28, 2003.

b. Relevant FAM sections include:

(1) 12 FAM 620, Unclassified Automated Information Systems;

(2) 12 FAM 630, Classified Automated Information Systems;

(3) 12 FAM 640, Domestic and Overseas Automated Information Systems Connectivity;

(4) 5 FAM 700, Internet and Intranet Use;

(5) 5 FAM 800, Information Systems Management;

(6) 12 FAM 540 Sensitive But Unclassified Information (SBU); and

(7) 3 FAM 4000 Employee Relations.

12 FAM 592 CYBER SECURITY INCIDENTS

(CT:DS-124; 01-10-2007)

As it relates to this program, a "cyber security incident" is a commission of an act against, or failure to protect, the Department of State's cyber infrastructure from potential damage or risk.

12 FAM 592.1 Cyber Security Infractions

(CT:DS-124; 01-10-2007)

a. A "cyber security infraction" is one subset of a cyber security incident that

contravenes computer security policy but does not result in damage to State's cyber infrastructure but may put the data or the system at risk. Cyber security infractions are often committed inadvertently; however, even inadvertent lapses or errors must be reported because they may cause an intrusion and unauthorized use. An unauthorized AIS user could:

(1) Introduce malicious material;

(2) Impersonate an authorized AIS user;

(3) Disrupt service in the Department's network; or

(4) Compromise the confidentiality of sensitive information.

b. Below is an all-inclusive list of incidents that *are* considered cyber security infractions.

(1) Disclosure of non-public key infrastructure (PKI) AIS user access passwords for an unclassified system:

(a) Passwords authenticate valid AIS users.

(b) Disclosing passwords defeats accountability by permitting an unauthorized AIS user to assume access for which there is no attribution. For example, an authorized method of granting another AIS user access to your e-mail account (when required) is to use the "permissions" function rather than sharing your AIS user account passwords.

(2) Attempts by an AIS user to obtain unauthorized access:

(a) AIS user accounts and data folders are protected to ensure confidentiality, availability, and integrity of the incorporated data.

(b) Access to a particular folder is determined by the data folder owner and/or granted by the system manager when it is created (e.g., AIS users attempting to access another user's data files within a data folder, for which an access restriction has been imposed).

(3) Unauthorized transfer of electronic data from unclassified systems to classified systems:

(a) Writeable disks and optical media that have been inserted in or connected to unclassified systems may not be inserted in or connected to classified systems without specific authorization.

(b) For more information on obtaining data transfer authorization, contact DS/SI/CS via email at ASKCS@state.gov.

(4) Failure to remove a crypto module (i.e., PKI smart card token) from

an individual workstation or server that is logged on could:

(a) Allow unauthorized AIS users to impersonate the rightful AIS user; and

(b) Undermine relationships of professional trust.

(5) Disclosure of a PKI password can:

(a) Permit an unauthorized AIS user to enter into a confidential relationship with an unsuspecting AIS user; and/or

(b) Enable falsely authenticated unauthorized AIS users to mimic true AIS users by falsely signing with digital signatures with access to such Sensitive But Unclassified (SBU) information as:

- Medical records,
- Personnel files, and/or
- Financial information meant for official use only.

12 FAM 592.2 Cyber Security Violations

(CT:DS-124; 01-10-2007)

a. A "cyber security violation," the second subset of a cyber security incident, is more serious than an infraction. It results in damage or significant risk to the Department's cyber infrastructure due to an individual's failure to comply with established Department computer security policy.

b. Below is an all-inclusive list of incidents that are considered cyber security violations.

(1) Deliberate introduction of malicious program code:

(a) Malicious program code (i.e., viruses, worms, Trojan Horses, and scripts) can deliver sophisticated attacks that spread rapidly throughout the Department's AIS causing damage to its cyber infrastructure, disrupting critical activities, and the Department's mission requirements.

(b) Excising viruses often involves shutting down the network, disrupting operations, and incurring significant costs.

(c) The Department attempts to protect the network from malicious program code by vigorously applying patches, managing firewalls, employing automatic virus protection, etc.; however, this only protects the network from previously identified threats.

(d) AIS users must also share in this responsibility by strictly

adhering to the Department's computer security policy. Failure to perform mandatory virus scans of electronic media introduced into the network via an auxiliary drive or downloading software/tools from known hacker Web sites are two examples that will be considered a deliberate act of non-compliance.

(2) Achieving or providing unauthorized administrator-level access:

(a) Affords the recipient unfettered access to restricted information and system security configuration and controls; and

(b) Compromises the integrity of the cyber infrastructure.

(3) Use of encryption to conceal an unauthorized act, such as the transfer of SBU to an unauthorized individual:

(a) Is an abuse of PKI privileges *(*Guidelines for determining authorized access to SBU are outlined in 12 FAM 543), and

(b) Demonstrates the sender's intent to conceal the unauthorized transmission.

(4) Introduction of unauthorized encryption.

(a) Unauthorized encryption refers to commercially available encryption software that enables the AIS user to send information through the Department's network to another AIS user with the same software bypassing system security configuration standards.

(b) The Department's PKI is the only encryption that may be operated on the Department's networks.

(5) Intentionally obtaining unauthorized AIS user-level access (e.g. receiving, pilfering, or obtaining another's password through social engineering, or hacking into a data folder for which an access restriction has been imposed) could:

(a) Violate, at a minimum, the integrity of the system security controls;

(b) Result in the loss of the resident information's confidentiality, integrity, and availability; and

(c) Put the data and the system at risk.

(6) Defeating or attempting to defeat security seals on Department information technology (IT) devices:

(a) Undermines the AIS user and the Department's reasonable assurance that no unauthorized person has tampered with the device; and

(b) Renders the device unverifiable from a security standpoint.

(7) Defeating or attempting to defeat cryptographic internal security measures of a crypto module (PKI smart card token):

(a) May enable AIS user access into areas where they are not authorized; and

(b) Could enable someone to assume another's identity, compromising the integrity of the Department's information and systems.

(8) Deliberate installation and/or initial activation of an unauthorized executable software application on a Department network.

(a) Installation and/or initial activation of unauthorized executable application software containing a virus or other malicious code could compromise the confidentiality, integrity, and availability of the network as well as the resident data. To prevent this type of compromise, all Department-owned software must be examined/tested and authorized by the Department's IT Change Control Board or Local Change Control Boards (IT CCB or Local CCBs) prior to installation or execution.

(b) The Bureau of Information Resource Management (IRM) maintains the complete listing of globally authorized software applications on their IT CCB Web site. For applications authorized on a local basis, see the Local CCB Web site.

(c) Systems administrators may install specialized software necessary for performing official business, but only after the IT CCB or local CCB has approved the software for use on Department AISs.

(d) Non-Department-owned application software, i.e. personally-owned, shareware, etc, is not authorized for installation/execution on the Department's networks.

(9) Connection of unauthorized hardware/electronic devices to Department networks.

(a) The Department goes to great lengths to manage its cyber vulnerabilities and inoperability issues with its vast array of computer equipment. Installing unauthorized computer equipment, such as laptops, routers, switches, and modems can defeat the system's established security measures, thus putting the system at risk.

(b) Unauthorized hardware/electronic devices are defined as:

(i) Department-owned hardware/electronic devices not

authorized by one of the Department's IT CCB or Local CCB, as appropriate for the specific system;

(ii) Department-owned hardware/electronic devices authorized by one of the IT CCB or local CCBs but not authorized for connection by the affected system owner or their representative; and,

(iii) Non-Department-owned hardware/electronic devices, i.e. personally-owned, contractor-owned, etc.

(10) Allowing unauthorized access or malicious modification to certificate authority servers, hardware cryptographic modules, or registration authority workstations subverts PKI functions necessary to ensure its confidentiality, integrity, and availability. For example, unauthorized access or malicious modification can invalidate electronic signatures and deny system encryption devices the ability to properly encrypt and decrypt when called upon.

(11) Installation of non-PKI hardware or software to certificate authority servers, cryptographic modules, or Registration Authority workstations can:

(a) Facilitate surreptitious system control, and

(b) Subvert the system manager's ability to assign and monitor the cryptographic and digital signature functions.

(12) Non-compliance with mandatory security configuration guidance.

(a) The Chief Information Officer (CIO) establishes a system configuration guidance that allows system managers and other information system security activities to conduct critical monitoring functions. Such monitoring protects the networks from intrusions and other malicious activities.

(b) Deviations from configuration guidance, unless specifically authorized by the CIO, could impair the Department's ability to secure its cyber infrastructure. If a need arises, IRM/IA, on behalf of the CIO, may waive configuration standards on a case-by-case basis.

12 FAM 592.3 Accessing Improper Internet Sites or Services

(CT:DS-124; 01-10-2007)

a. As described in 5 FAM 723, Department policy prohibits **AIS users** from deliberately accessing improper Internet sites or services. Such activities by themselves will not be considered a cyber security incident; however

access to such sites may put the security of the Department's cyber infrastructure unnecessarily at risk. Therefore, DS will investigate these events to determine if a cyber security incident (see 12 FAM 592.3(b), below) or criminal act has occurred as a result of the visitation to an improper site.

b. If DS/IS/APD determines a cyber security violation has occurred as a result of this prohibited activity, i.e., malicious code downloaded or unauthorized program was installed or executed, etc., they will process the incident under the Cyber Security Incident Program.

c. Once DS/IS/APD determines that no cyber security violation has occurred, they will conclude their investigation and will forward a summary of investigative findings to the Bureau of Human Resources' Office of Employee Relations (HR/ER).

d. DS/SI/IS will forward summaries for activities involving contractors to the applicable contracting officer and parent company. DS/IS/APD will forward summaries for tenant agency personnel to their parent agency.

12 FAM 592.4 Reporting Cyber Security Incidents

(CT:DS-124; 01-10-2007)

a. Reporting cyber security incidents is every employee's responsibility, so all personnel must be familiar with the list of cyber security infractions and violations in 12 FAM 592. Employees must inform their ISSO and DS/IS/APD, the Regional Security Office (RSO) abroad, or their Bureau Security Officer (BSO) domestically, of any improper cyber security practice that comes to their attention, so remedial action may be taken.

b. Cyber security incidents may also be detected and reported in the following manner:

(1) During the normal course of their duties, ISSOs will report cyber security events, i.e. anomalies and other suspicious activities, to DS' Computer Incident Response Team (CIRT). DS/IS/APD coordinates daily with the CIRT, collecting and analyzing their data to determine which cyber security events should be investigated as cyber security incidents. When possible cyber security incidents are identified, DS/IS/APD will contact the appropriate RSO or BSO and advise them to initiate a cyber security investigation.

(2) When the RSO or BSO identifies a possible cyber security incident, they will immediately notify DS/IS/APD, the ISSO, and initiate a cyber security investigation.

(3) When the ISSO identifies a possible cyber security incident they will immediately notify the RSO or BSO, as appropriate, and IRM/IA and the CIRT. Regional Computer Security Officers may also report

cyber security incidents to the ISSO and/or RSO, as appropriate.

12 FAM 592.5 Investigating and Processing Cyber Security Incidents

(CT:DS-124; 01-10-2007)

a. The RSO abroad or BSO domestically, or DS/IS/APD if no BSO is assigned, herein referred to as "the investigator," will investigate cyber security incidents. The investigator will likely require technical assistance from the ISSO or system manager. The investigation will attempt to determine:

   (1) The extent of the incident,

   (2) If a criminal act has occurred (in which case it will be referred to DS/CR/CIF and evidence preserved),

   (3) Possible or actual damage to the network,

   (4) Mitigating and aggravating factors, and

   (5) Identity of individual(s) culpable for the incident.

b. Suggestions for capturing cyber security incident investigative elements, as well as Form OF-118, Record of Incident, are posted in the CSIP Toolkit.

c. When the Investigator has collected sufficient information to conclude the investigation:

   (1) The investigator will prepare a Form OF-118, Record of Incident, completing the header information and Part 1b – Cyber Security Incidents Only.

   (2) The investigator should present the Form OF-118 to the AIS user for execution of his/her portion of Part 2 – Statement of Person Suspected of Incident, and his/her signature and discuss its contents and ramification. Form OF-118 allows the AIS user to provide any mitigating factors, such as lack of culpability, which he/she believes would be pertinent to the adjudication process.

   (3) AIS user shall return the signed Form OF-118 to the investigator as soon as possible, but not later than 3 working days. If the AIS user fails or refuses to sign the form within 3 working days, the investigator will document this fact in the security officer comments on Form OF-118, item 3, Comments of Unit/Post/Regional Security Officer.

   (4) The investigator will then give the Form OF-118 to the AIS user's immediate supervisor for review and signature.

d. After the supervisor has signed and returned the form:

   (1) The investigator will complete item 3, reporting the results of the investigation in a brief summary, indicating whether the AIS user should be a held accountable for this cyber security incident.

   (2) The investigator will submit their investigative findings, any additional support documentation, and the Form OF-118 to DS/IS/APD for adjudication.

e. At a constituent post, the post security officer (PSO) may perform these duties on behalf of the RSO and forward all investigative documentation and the Form OF-118 to the responsible RSO.

f. Upon request, the investigator must provide a copy of the completed Form OF-118 to the person(s) alleged to be responsible for the incident.

g. If, as part of the cyber security incident investigation, an employee is to be personally interviewed, is a member of a collective bargaining unit for which a union representative has exclusive representation rights, and the employee reasonably believes that the interview may result in disciplinary action against him/her, the investigating official shall give the employee the opportunity to be represented by the inclusive representative, if the employee so requests. This right is known as the Weingarten Right. When the employee invokes the Weingarten Right, the investigating official will allow a reasonable amount of time for a union representative to attend the interview.

12 FAM 593 EVALUATION OF CYBER SECURITY INCIDENTS

(CT:DS-124; 01-10-2007)

a. DS/IS/APD performs evaluation and adjudication of all reported cyber security incidents to determine:

   (1) The validity/invalidity of reported CSIP incidents;

   (2) Whether there are CSIP infractions or violations;

   (3) Whether further CSIP action is required; and

   (4) Who is culpable for the CSIP incidents.

b. AIS users will be held accountable for their individual actions. If supervisors are aware of subordinates committing cyber security incidents and allow the conduct to continue, they may also be held responsible for failure to provide effective organizational security oversight. This might occur, for example, when a supervisor allows subordinates to connect unauthorized hardware to the network or install privately owned software

on U.S. Government computers.

c. When the cyber security incident investigation does not warrant charging a specific individual, DS/IS/APD may still adjudicate the incident as valid without holding a specific individual accountable.

   (1) Mitigating circumstances may prevent narrowing responsibility to an individual AIS user; and

   (2) The DS/SI/IS Office Director must approve this type of adjudication.

d. Upon completion of the adjudication, DS/IS/APD will notify in writing the culpable individual*(s)* charged during the investigation of the adjudication results specific to them. DS/IS/APD will also notify the appropriate RSO, BSO, or principal unit security officer (PUSO), who will provide a copy to the individual's supervisor.

12 FAM 594 APPEALS

(CT:DS-124; 01-10-2007)

a. An AIS user may appeal the validity of and/or his/her culpability in a cyber security incident by submitting the appeal, in writing, to the Division Chief, DS/IS/APD. This appeal request must be done immediately after receiving written notification that DS/IS/APD has adjudicated the incident.

   NOTE: An AIS user's statement on Form OF-118 is considered part of the initial adjudication, and does not constitute an appeal.

b. DS/IS/APD will forward the appeal request, along with any other pertinent data, to the DS/SI/IS Office Director for an appeal decision.

12 FAM 595 ADMINISTRATIVE ACTIONS

12 FAM 595.1 Record Keeping and Administrative Action Framework

(CT:DS-124; 01-10-2007)

a. DS/IS/APD will maintain cyber incident investigation and adjudication files and documentation on all personnel, who have incurred cyber security incidents. Information from these files will be made available to the Director General of the Foreign Service and Director of Human Resources (M/DGHR) or other appropriate State Department officials with a need-to-know, as may be needed for deliberation of nominations or other personnel decisions. Cyber security incident information will be included

in Single-Scope Background investigation reports on candidates for Presidential appointments, and may be disseminated to relevant others consistent with the Privacy Act and other governing law. Upon an employee's termination, the records will be retired.

b. At posts abroad, a record of each security incident must be kept on file for at least 36 months. The record, which may be destroyed after 36 months, should include a copy of the:

(1) Completed Form OF-118,

(2) Signed reply from the AIS user acknowledging that he or she understands the policies and ramifications of future incidents,

(3) Completed technical checklist, and

(4) All technical supporting documentation.

c. Cyber security incidents referred to HR/ER for disciplinary action will be handled on a case-by-case basis, but in principle, disciplinary action will become progressive following additional incidents.

d. An AIS user's adverse cyber security incident history may result in the curtailment of a current assignment or denial of future assignments.

12 FAM 595.2 Referral for Disciplinary Action and Security Clearance Review Related to Cyber Security Infractions (Department Employees)

(CT:DS-161; 03-01-2011)

After affirmative adjudication by DS/IS/APD of cyber security infraction(s) within the current 3-year moving window (see 12 FAM 090 definition), DS/IS/APD will take the following actions:

(1) First infraction—The DS/IS/APD Division Chief will send a letter of warning to the employee that requires a signed reply acknowledging that the employee understands the policies and ramifications of future security incidents.

(a) The employee's supervisor must provide counseling to the employee stressing the seriousness of the Department's cyber security policies.

(b) The ISSO and RSO or post security officer (PSO) abroad, or BSO/USO domestically, will provide the employee with remedial instruction and advice regarding cyber security.

(2) Second infraction—The DS/IS/APD Division Chief will send a letter of warning to the employee that includes a statement concerning actions DS will take in the event of future cyber security infractions.

(a) This warning notification requires a signed reply acknowledging that the employee understands the policies and ramifications of future security incidents.

(b) The ISSO and RSO or PSO abroad, or BSO/USO domestically, will provide the employee with remedial instruction and advice regarding cyber security.

(3) Third infraction—Letter of Caution. The DS/SI Senior Coordinator for Security Infrastructure will send a letter of caution to the employee that includes a statement concerning the actions DS will take in the event of future cyber security infractions.

(a) The letter of caution requires a signed reply acknowledging that the employee understands the policies and ramifications of future incidents.

(b) The system manager will suspend the employee's AIS access until the ISSO retrains and retests the employee on proper AIS procedures.

(4) Fourth infraction—After affirmative adjudication and determination that a fourth and/or subsequent infraction within the current 3-year window has occurred, the DS/IS/APD Division Chief will send a letter informing the employee that in the event an appeal of the infraction is denied or not submitted within 30 calendar days:

(a) DS/IS/APD will refer a Report of Investigation to HR/ER for appropriate disciplinary action, which includes:

- All infractions occurring "within the current 3-year moving window;"
- Any mitigating or aggravating factors; and,
- Other valid cyber and information security incidents under 12 FAM 550.

(b) The letter will also include a statement concerning actions DS will take in the event of future cyber security infractions; and, requires a signed reply acknowledging that the employee understands the policies and ramifications of future security incidents.

NOTE: The ISSO and RSO or PSO abroad, or BSO/USO domestically, will provide the employee with remedial instruction and advice regarding cyber security.

(c) DS/IS/APD will forward referrals for disciplinary action of locally employed staff (*LE staff*) (when authority for that remains at post) to the RSO for delivery to the HR office at post.

(d) For cleared personnel, DS/IS/APD will refer the matter to the Director of the Office for Personnel Security and Suitability (DS/SI/PSS) for taking appropriate action relating to their security clearances.

(e) The system manager will suspend the employee's AIS access until the ISSO retrains and retests the employee on proper AIS procedure.

12 FAM 595.3 Referral for Actions Related to Cyber Security Violations (Department Employees)

(CT:DS-161; 03-01-2011)

a. After affirmative adjudication by DS/IS/APD that a cyber security violation has occurred and culpability is assigned, DS/IS/APD will refer the investigation report to DS/SI/PSS and HR/ER for appropriate action. The report must include a summary of mitigating or aggravating factors, and a list of other valid cyber and information security incidents under 12 FAM 550.

b. DS/IS/APD will forward referrals for disciplinary action of locally employed staff (*LE staff*) (when authority for that remains at post) to the RSO for delivery to the HR office at post.

c. The system manager will suspend the employee's AIS access until the ISSO retains and retests the employee on proper AIS procedure.

12 FAM 595.4 Referral for Actions Related to Cyber Security Incidents (Other Agencies' Employees)

(CT:DS-124; 01-10-2007)

a. Cyber security incidents involving employees of other Federal agencies or organizations or their contractors are reported in the same manner as described herein (see 12 FAM 592). RSOs and ISSOs abroad must coordinate reporting all such incidents, including processing Form OF-117, Notice of Security Incident, and Form OF-118, Record of Incident, to DS/IS/APD. DS/IS/APD will coordinate any further investigation.

b. The system manager will suspend the employee's AIS access upon each occurrence of a cyber security violation as well as the third and subsequent infractions in the current 3-year moving window until the ISSO retrains and retests the employee on proper AIS procedure.

12 FAM 595.5 Referral for Actions Related to Cyber Security Incidents (Personal Services and Commercial Contractors)

(CT:DS-124; 01-10-2007)

a. DS/IS/APD will forward copies of Form OF-117, Form OF-118, and the documented results of any investigation to the contractor's facility security officer for appropriate action and to the Office of Information Security, Industrial Security Division (DS/IS/IND).

b. DS/IS/IND will advise the Department's contracting officer representative (COR) of the nature and seriousness of the incident, and will provide details of any derogatory information to the cognizant security clearance investigative authority.

c. The system manager will suspend the contractor's AIS access upon each occurrence of a cyber security violation, and also for the third and subsequent infractions in the current 3-year moving window, until the ISSO retrains and retests the contractor on proper AIS procedure.

12 FAM 596 CRIMINAL LAWS

(CT:DS-116; 11-01-2005)

Incidents involving intentional risk or damage to U.S. Government AISs may be subject to criminal penalties.

12 FAM 597 THROUGH 599 UNASSIGNED